Performance Analysis of Switches in High Speed LAN

Muhammad Imran, Asif Shaikh, Syed S. Rizvi, Khaled M. Elleithy
Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT
{mimran, ashaikh, srizvi, elleithy}@bridgeport.edu

Abstract-**This paper presents an analysis of switches in high speed LAN. In order to support our analysis, this paper provides both analytical and mathematical models. The proposed analytical model is based on a finite state Markov model developed for analyzing networks with virtual channels in a switched LAN. Our proposed mathematical model provides a mean to quantify different critical parameters such as end-to-end delay, short and long message latency, channel bandwidth, and utilization in switched LAN. Simulation is performed using OPNET that based on the mathematical expressions derived in the mathematical model. In addition, simulation results of this paper compare the performance of high speed LAN with respect to the utilization of both switches and hub. Finally, based on the simulation results, we provide a performance analysis that indicates the role of each critical parameter in the overall perfor.**

I. Introduction

Switches and net works A typical net work consists of nodes and computer a medium for connection, either wired or wireless Special network equipment, such as routers or hubs In the case of the Internet, these pieces work together to allow your computer to send information to another computer .The other computer can be on the other side of the world. Switches are a fundamental part of most networks.

Switch enable several users to send information over a net work Users can send the information at the same time and do not slow each other down .just like routers allow different networks to communicate with each other, switches allow different nodes of a connection point, typically a computer .Switches allow the nodes to communicate in a smooth and efficient manner.

There are many different types of switches and network, LAN switches. Essentially, LAN switches create Series of instant networks that contain only the two devices that communicate with each other at that particular moment. This document focuses on Ethernet networks that use LAN switches. The document describes what a LAN switch is and how transparent bridging works. The document also explains VLANs, trucking, and spanning trees.

In the most basic type of network of today, nodes simply connect together with the use of bus. As a network grows, there are some potential problems with this configuration scalability In a hub network, there is a limit to the amount of bandwidth that users can share.

Significant growth is difficult to accommodate without a sacrifice in performance. Applications today need more bandwidth than ever before. Quite often the entire network must undergo a periodic redesign to accommodate growth latency latency is the amount of time that a packet takes to get to the destination. Each node in a hub-based network has to wait for an Opportunity to transmit in order to avoid collisions.

The latency can increase significantly as you add more nodes or if user transmits a large file across the network. All the other nodes must wait farina opportunity to send packets. You have probably experienced this problem before at work. You try to access a server or the internet, and suddenly everything slows down to a crawl.

Network Failure- In a typical network, one device on a hub can cause problems for other devices that attach to the hub. Incorrect speed setting or excessive broadcasts cause the problems. An example of an incorrect speed setting is 100Mbos on a 10Mbps hub You can configure switches to limit broadcast levels.

Collisions – Ethernet uses a process with the carrier sense multiple access collision detect (CSMA/CD) to communicate across the network. Under CSMA-CD, a node does send out a packet unless the, collision occur and the packets are lost then, both nodes wait for a random amount of time and retransmits the packets. Any part of the network where packets from two or more nodes can interfere with each other is a collision domain.

A network with a large number of nodes on the same segment often has a lot of collision and, therefore, large Collision domain. Hubs provide an easy way to scale up and shorten the distance that the packets must travel to get from one node to another .But hubs do not break up the actual network into discrete segments. Switch handles this job.

Think of a hub as a four-way intersection where all vehicles have to stop. If more than one car reaches the intersection at one time, the cars must wait for a turn to proceed. But a switch is like a cloverleaf intersection. Each car can take an exit ramp to get to the destination without the need to stop and wait for other traffic to pass. Now imagine this scenario with a dozen or even a hundred roads that intersect at a single point. The wait and the potential for a collision increase significantly if every car has to check all the other roads before the car proceeds. Imagine that you can take an exit ramp from any one of those roads to the road of your choice. This ability is what a switch provides for network traffic.

II. RELATED WORK

There is a vital difference between a hub and a switch; all the nodes that connect to a hub share the bandwidth, but a device that connects to a switch port has the full bandwidth alone. For example, consider 10 nodes that communicate with use of a hub on a 10 Mbps network. Each node can only get a portion of the 10 Mbps if other nodes on the hub want to communicate as well. But, with a switch, each node can possibly communicate at the full 10 Mbps. Consider the road analogy. If all the traffic comes to a common intersection, the traffic must share that intersection. But a cloverleaf allows all the traffic to continue at full speed from one road to the next.

In a fully switched network, switches replace all the hubs of an Ethernet network with a dedicated segment for every node. These segments connect to a switch, which supports multiple dedicated segments. Sometimes the number of segments reaches the hundreds. Since the only devices on each segment are the switch and the node, the switch picks up every transmission before the transmission reaches another node. The switch then forwards the frame over the appropriate segment. Since any segment contains only a single node, the frame only reaches the intended recipient. This arrangement allows many conversations to occur simultaneously on a network that uses a switch.

Switching allows a network to maintain full-duplex Ethernet. Before switching existed, Ethernet was half duplex. Half duplex means that only one device on the network can transmit at any given time. In a fully switched network, nodes only communicate with the switch and never directly with each other. In the road analogy, half duplex is similar to the problem of a single lane, when road construction closes one lane of a two-lane road. Traffic attempts to use the same lane in both directions. Traffic that comes one way must wait until traffic from the other direction stops in order to avoid collision.

Fully switched networks employ either twisted pair or fiber-optic cable setups. Both twisted pair and fiber-optic cable systems use separate conductors to send and receive data. In this type of environment, Ethernet nodes can forgo the collision detection process and transmit at will; these nodes are the only devices with the potential to access the medium. In other words, the network dedicates a separate lane to traffic that flows in each direction. This dedication allows nodes to transmit to the switch at the same time that the switch transmits to the nodes. Thus, the environment is collision-free. Transmission in both directions also cans effectively double the apparent speed of the network when two nodes exchange information. For example, if the speed of the network is 10 Mbps, each node can transmit at 10 Mbps at the same time.

Most networks are not fully switched because replacement of all the hubs with switches is costly. Instead, a combination of switches and hubs create an efficient yet cost-effective network. For example, a company can have hubs that connect the computers in each depart\nt and a switch that connects all the department-level hubs together.

III. AN EFFECTIVE SOLUTION FOR HIGH SPEED LANS

A. *Proposed Switching Technology*

A switch has the potential to radically change the way that the nodes can communicate with each other. But what makes a switch different than a router? Switches usually work at **Layer 2 (Data or Datalink)** of the Open System Interconnection (OSI) reference model with use of MAC addresses. Routers work at **Layer 3 (Network)** with Layer 3 addresses. The routers use IP, Internetwork Packet Exchange (IPX), or Appletalk, which depends on the Layer 3 protocols that are in use. The algorithm that switches use to decide how to forward packets is different than the algorithms that routers use to forward packets. One difference in the algorithms is how the device handles **broadcasts**.

On any network, the concept of a broadcast packet is vital to the operability of the network. Whenever a device needs to send out information but does not know to whom to send the information, the device sends out a broadcast. For example, every or time a new computer other device comes onto the network, the device sends out a broadcast packet to announce the entry. The other nodes, such as a domain server, can add the device to the **browser list**. The browser list is like an address directory. Then, the other nodes can communicate directly with that device. A device can use broadcasts to make an announcement to the rest of the network at any time.

LAN switches rely on **packet switching**. The switch establishes a connection between two segments and keeps the connection just long enough to send the current packet. Incoming packets, which are part of an Ethernet frame, save to a temporary memory area. The temporary memory area is a **buffer**. The switch reads the MAC address that is in the frame header and compares the address to a list of addresses in the switch **lookup table**. In a LAN with an Ethernet basis, an Ethernet frame contains a normal packet as the payload of the frame. The frame has a special header that includes the MAC address information for the source and destination of the packet.

Switches use one of three methods for routing traffic:

- Cut-through
- Store and forward
- Fragment-free

Cut-through switches read the MAC address as soon as a packet is detected by the switch. After storing the six bytes that make up the address information, the switches immediately begin to send the packet to the destination node, even though the rest of the packet is coming into the switch.

A switch that uses **store and forward** saves the entire packet to the buffer and checks the packet for Cyclic Redundancy Check (CRC) errors or other problems. If the packet has an error, the packet is discarded. Otherwise, the switch looks up the MAC address and sends the packet on to the destination node. Many switches combine the two methods by using cut-through until a certain error level is reached, then changing over to store and forward. Very few switches are strictly cut-through because this provides no error correction.

A less common method is **fragment-free**. Fragment-free works like cut-through, but stores the first 64 bytes of the packet before sending the packet on. The reason for this is that most errors and all collisions occur during the initial 64 bytes of a packet.

LAN switches vary in physical design. Currently, there are three popular configurations in use:

- **Shared-memory**—The switch stores all incoming packets in a common memory buffer that all the switch **ports** (input/output connections) share. Then, the switch sends the packets out the correct port for the destination node.
- **Matrix**—This type of switch has an internal grid with which the input ports and the output ports cross each other. When the switch detects a packet on an input port, the switch compares the MAC address to the lookup table to find the appropriate output port. The switch then makes a connection on the grid where these two ports intersect.
- **Bus-architecture**—Instead of a grid, an internal transmission path (**common bus**) is shared by all the ports using time division multiplex access (TDMA). A switch with this configuration dedicates a memory buffer to each port. There is an application-specific integrated circuit (ASIC) to control the internal bus access.
- **Transparent Bridging—**Most Ethernet LAN switches use transparent bridging to create the address lookup tables. Transparent bridging technology allows a switch to learn everything that the switch needs to know about the location of nodes on the network without the need for the network administrator to do anything. Transparent bridging has five parts:

- Learning
- Flooding
- Filtering
- Forwarding
- Aging

The addition of the switch to the network occurs, and the various segments plug into the switch ports.

- The computer Node A on Segment A sends data to the computer Node B on another segment, Segment C.
- The switch gets the first packet of data from Node A. The switch reads the MAC address and saves the address to the lookup table for Segment A. The switch now knows where to find Node A whenever a packet with this address arrives. This process is **learning**.
- Since the switch does not know where Node B is, the switch sends the packet to all the segments. But the switch does not send the packet to the segment on which the packet arrived, Segment A. When a switch sends a packet out to all segments to find a specific node, this is **flooding**.
- Node B gets the packet and sends a packet back to Node A in acknowledgement.
- The packet from Node B arrives at the switch. Now the switch can add the MAC address of Node B to the lookup table for Segment C. Since the switch already knows the address of Node A, the switch sends the packet directly to the node. Because Node A is on a different segment than Node B, the switch must connect the two segments to send the packet. You call this action **forwarding**.
- The next packet from Node A to Node B arrives at the switch. The switch now has the address of Node B, too, so the switch forwards the packet directly to Node B.
- Node C sends information to the switch for Node A. The switch looks at the MAC address for Node C and adds the address to the lookup table for Segment A. The switch already has the address for Node A and determines that both nodes are on the same segment. The switch does not need to connect Segment A to another segment for the data to travel from Node C to Node A. Therefore, the switch ignores packets that travel between nodes on the same segment. This is **filtering**.
- The switch continues to learn and flood as it adds nodes to the lookup tables. Most switches have plenty of memory to maintain the lookup tables. But remove old information so that the switch does not waste time with a search through stale addresses. In order to optimize the use of this memory, switches use the **aging** technique.

B. *Proposed Analytical Model*

For a switch with N ports of the same bit rate, the result is that the aggregate bandwidth approaches to a switch with "N" segments or ports. Total Band width in the switch is used by every user without sharing the band. This can be expressed as:

$$\text{Band Width} = BW = N * (\text{media - bit-rate})/2$$

When connected directly to a switching **LAN** station may operate in full duplex mode, access control is not necessary. If all the stations use full duplex mode, the aggregate switch bandwidth approaches,

$$BW = N * (\text{media - bit-rate})$$

For example, consider 10 nodes that communicate with use of a hub on a 10 Mbps network. Each node can only get a portion of the 10 Mbps if other nodes on the hub want to communicate as well. But, with a switch, each node can possibly communicate at the full 10 M bps. Consider the road analogy. If all the traffic comes to a common intersection, the traffic must share that intersection. But a cloverleaf allows all the traffic to continue at full speed from one road to the next

In the example, two nodes share each segment. In an ideal LAN-switched network, every node would have a separate segment. Separate segments would eliminate the possibility of collisions and the need for filtering. Notice that, while a node on Segment A talks to a node on Segment B at 10 Mbps, a node on Segment C can also communicate with a node on Segment B at 10 Mbps.

IV. Simulation Results

For the sake of simulation, we have setup a local area networks which is interconnected by switches

A. Main Objectives

This lab has been designed to demonstrate the implementation of switched local area networks. The simulation in this lab will help examine the performance of different implementations of local area networks connected by switches and hubs.

There is a limit on the number of hosts that can be attached to a single network and on the size of a geographic area that a single network can serve [3, 4]. Computer networks use switches to enable the communication between one host and another, even when no direct connection exists between those hosts [3].

The key problem that a switch must deal with is the finite bandwidth of its outputs [4]. If packets destined for a certain output arrive at a switch and their arrival rate exceeds the capacity of that output, then we have a problem of connection. In this case, the switch will queue (or buffer) packets until the contention subsides. If it lasts too long, however, the switch will run out of buffer space and be forced to discard the packets. When packets are discarded too frequently, the switch is said to be congested [3].

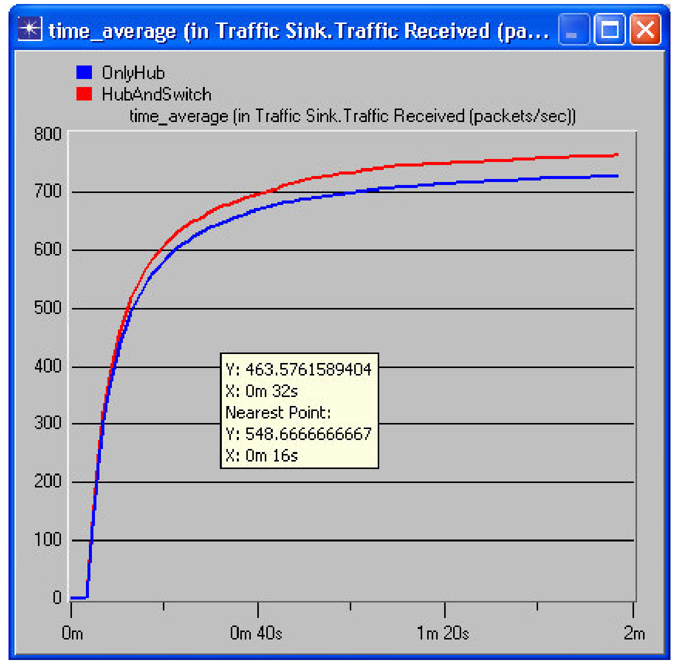

Fig. 1. Traffic Received (Throughput) for the Hub and Hub-and-Switch Cases.

B. The Analysis of Switch in LAN

The following study demonstrates why the adding of a switch makes a network perform better in terms of throughput and delay characteristics.

We have studied two cases: (1) Ethernet with the hub only, and (2) Ethernet with the hub and switch. The results shown in Figures 1 and 2 demonstrate that, although the traffic send is almost the same in both cases, the traffic received has improved in the Hub-and-Switch case. The second configuration makes

network performs better in terms of throughput and delay characteristics. With a switched network any user can be connected to each port directly [3]. Therefore, the bandwidth is shared only among a number of users in the workgroup (connected to the ports). Since this is the reduced media, the sharing of other portions of the bandwidth is available. Switches can also maintain multiple connections at one point [3, 4].

Switches normally have higher port counts than bridges and divide network into several dedicated channels independent ("parallel") from each other. These multiple independent data paths increase the throughput capacity of a switch. There is no contention to gain access, and LAN switch architecture becomes scalable. Another advantage of switches is that most of them are self-configuring. This property allows to minimizing the network downtime, although ways for manual configuration are also available [4].

C. Analysis of Collisions in the Switched Network

The use of the switch makes it possible to reduce the collisions on the network. The communication procedures follow the certain rules. For example, when a peripheral device wishes to communicate, it sends the request for communication (a "message") that reaches the switch. If another peripheral device

Communicates already, two messages are found at the same time on the network. The message from the first host is taken

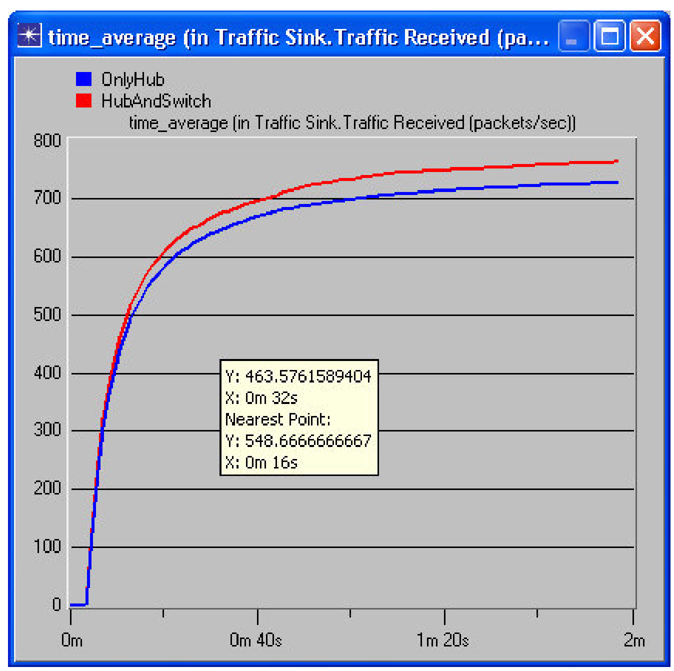

Fig. 2. Traffic Sent (Load) for the Hub and Hub-and-Switch Cases.

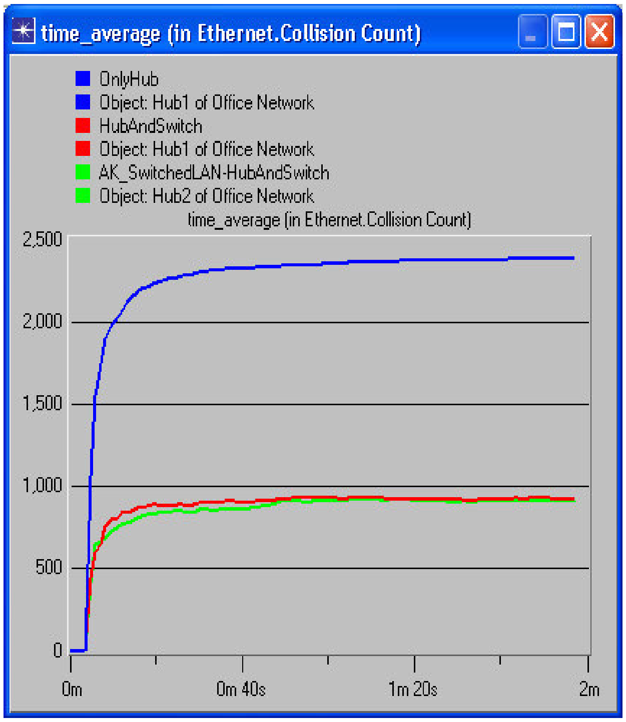

Fig. 3. Collision Counts for Various Ethernet Network Configurations.

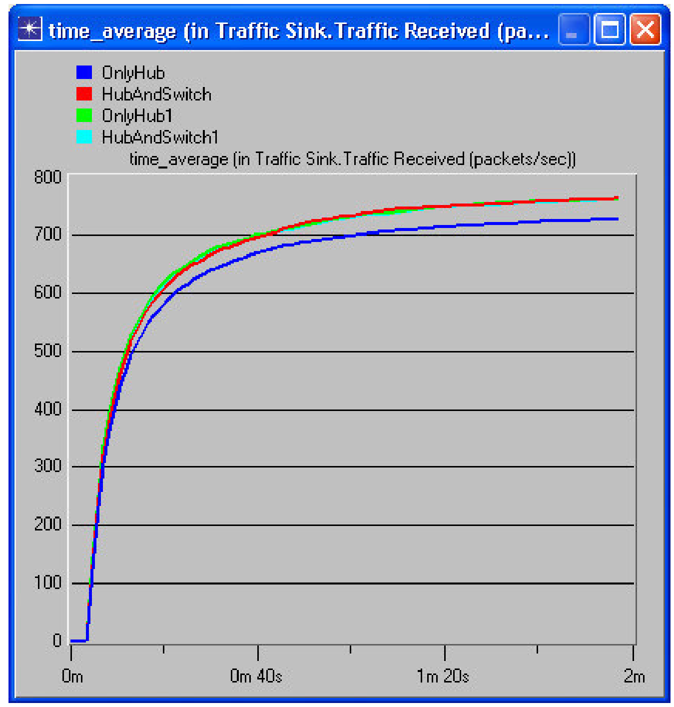

Fig. 5. Time Average in Traffic Received

at the beginning of a queue, and the second host waits for trying again to communicate a few milliseconds later. Switches upon finding that the destination port is overloaded will send

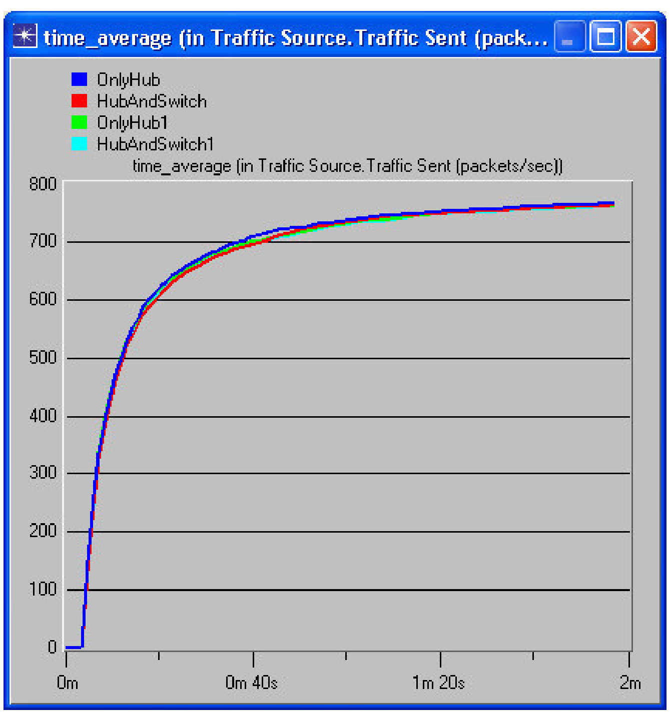

Fig. 4. Time Average in Traffic Sent

the *jam* message to the sender. Since the decoding of the MAC address is fast and the switch can, in very little time, respond with a *jam* message, collision or packet loss can be avoided [3, 4]. The data shown in Figure 3 demonstrates that the network performance improves in LANs, in which LAN switches are installed, because the LAN switch creates isolated collision domains. Many LAN switch installations assign just one user per port [3]. By distributing users over several collision domains, collisions are avoided and performance improves.

We have studied the network performances (in terms of delay throughput and collision count) for the following four network configurations:

- The Only-Hub case: Hubs without any switch.
- The Only-Hub1case: Hub is replaced by a switch
- The Hub-and-Switch case: Two hubs and one switch
- The Hub-and-Switch1 case: Two switches only

The Traffic Sent (load) parameters have been almost the same in all the cases (see Figure 4). We have found that there is a slight improvement in the network performance (Traffic Received characteristics) in all the cases with switches (see Figure 5).

The data shown in the Figure 6 demonstrates that the delay in the cases with the switches without hubs (the Only-Hub1, Hub-and-Switch, and Hub-and-Switch1 cases) is significantly less compared to the network configurations with a hub (the Only-Hub case). Particularly, when we replaced two hubs with switches the delay is almost negligible.

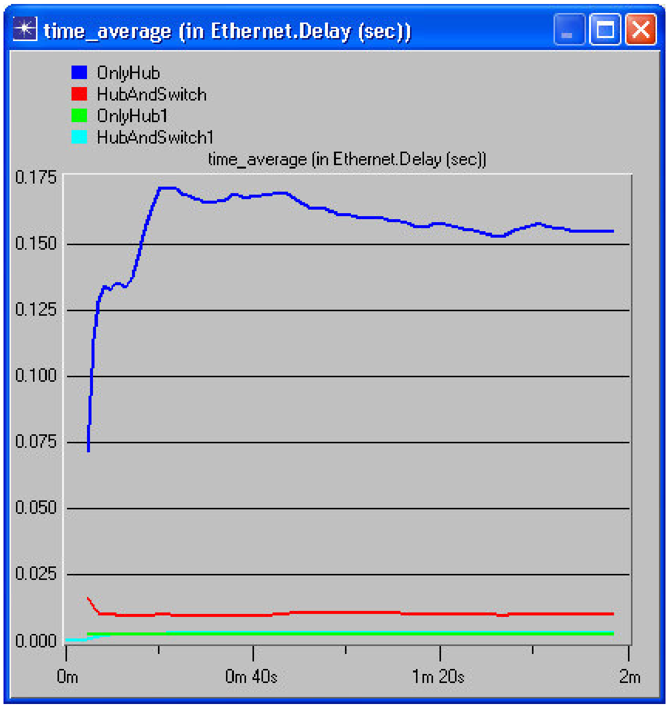

Fig. 6. Time Average Delay for Various Network Configurations

CONCLUSION

This paper presents a simulation based analysis of high-speed LANS by using hub and switches. By using switch, we can come up with required solutions for the problems arouse by hubs and routers in network. In this paper, we presented the mathematical solution and simulation results for the switch LAN with different network configurations.

REFERENCES

[1] Internet Engineering Task Force (IETF), "RFC 1577,
[2] Classical IP and ARP Over ATM", January 1994.
[3] FDDI Synchronous Forum, "FDDI Synchronous Forum
[4] Implementers' Agreement, Revision 2", 1 December 1993.
[5] "A New High Speed Data Transfer AAL", TlSl working group proposal, 8 November 1991.
[6] The ATM Forum, "ATM User Network Interface, Version
[7] (UN13.1) Specification ", draft of 28 May 1994.
[8] The ATM Forum, "ATM User Network Interface, Version
[9] (UN13.1) Specification ", draft of 28 May 1994.